

WHAT IS CLAIMED IS:

1 1. A login method comprising  
2 processing a login token, if provided, during a login attempt, wherein the login  
3 attempt is impermissible, and thus unsuccessful, if the login attempt occurs before expiration  
4 of a first period of time following an unsuccessful login attempt associated with said login  
5 token; and  
6 providing an updated login token in response to the login attempt, wherein the  
7 updated login token does not permit a subsequent login attempt before expiration of a second  
8 period of time if the login attempt is unsuccessful.

1 2. The login method of claim 1, further comprising  
2 maintaining a login-attempt success indicator, said login-attempt success indicator  
3 indicating whether the login attempt is successful, said login-attempt success indicator being  
4 referenced during the subsequent login attempt

1 3. The login method of claim 2, further comprising  
2 including in the updated login token an attempt success indicator, said attempt success  
3 indicator indicating whether the login attempt is successful, said attempt success indicator  
4 being referenced during the subsequent login attempt.

1 4. The login method of claim 3, wherein  
2 the login-attempt success indicator is a login class, wherein the login class is first-  
3 class if the login attempt is successful.

1 5. The login method of claim 1, further comprising  
2 maintaining a time stamp, said time stamp corresponding to the second period of time.

1 6. The login method of claim 1, further comprising  
2 inserting in the updated login token a time stamp, said time stamp corresponding to  
3 the second period of time.

1 7. The login method of claim 1, further comprising  
2 maintaining an account identifier, said account identifier corresponding to an account  
3 that is the subject of the login attempt, wherein the subsequent login attempt is impermissible  
4 if an account that is the subject of the subsequent login attempt does not correspond to the  
5 account identifier.

1 8. The login method of claim 1, further comprising  
2 inserting in the updated login token an account identifier, said account identifier  
3 corresponding to an account that is the subject of the login attempt, wherein the subsequent  
4 login attempt is impermissible if an account that is the subject of the subsequent login attempt  
5 does not correspond to the account identifier.

1 9. The login method of claim 1, further comprising  
2 maintaining a network address identifier, said network address identifier  
3 corresponding to a network address from which the login attempt originates, wherein the  
4 subsequent login attempt is impermissible if a network address from which the subsequent  
5 login attempt originates does not correspond to the network address identifier.

1 10. The login method of claim 1, further comprising  
2 inserting in the updated login token a network address identifier, said network address  
3 identifier corresponding to a network address from which the login attempt originates,  
4 wherein the subsequent login attempt is impermissible if a network address from which the  
5 subsequent login attempt originates does not correspond to the network address identifier.

1 11. The login method of claim 1, further comprising  
2 maintaining a password identifier, said password identifier corresponding to a  
3 password submitted with the login attempt, wherein the subsequent login attempt is  
4 impermissible if a password submitted with the subsequent login attempt does not correspond  
5 to the password identifier.

1 12. The login method of claim 1, further comprising

2 inserting in the updated login token a password identifier, said password identifier  
3 corresponding to a password submitted with the login attempt, wherein the subsequent login  
4 attempt is impermissible if a password submitted with the subsequent login attempt does not  
5 correspond to the password identifier.

1 13. The login method of claim 1, further comprising  
2 inserting in the updated login token a validity stamp, said validity stamp designed to  
3 prevent the use of an invalid login token, wherein the login attempt is impermissible if the  
4 login token does not include a valid validity stamp.

1 14. The login method of claim 1, further comprising  
2 inserting in the updated login token a nonce, said nonce designed to prevent the reuse  
3 of an otherwise valid login token, wherein the login attempt is impermissible if the login  
4 token does include a nonce used in a prior login attempt.

1 15. The login method of claim 1, further comprising  
2 maintaining a count of unsuccessful login attempts.

1 16. The login method of claim 15, further comprising  
2 incrementing the count if the login attempt is impermissible.

1 17. The login method of claim 15, further comprising  
2 incrementing the count if the login attempt is permissible but otherwise unsuccessful.

1 18. The login method of claim 15, further comprising  
2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined  
4 threshold.

1 19. The login method of claim 15, further comprising

2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined threshold  
4 within a third period of time.

1 20. The login method of claim 1, wherein  
2 the login attempt is impermissible if the login token is not provided during the login  
3 attempt.

1 21. The login method of claim 1, further comprising  
2 maintaining a count of unsuccessful login attempts to login with a password.

1 22. The login method of claim 21, further comprising  
2 incrementing the count if the login attempt is impermissible and is made with the  
3 password.

1 23. The login method of claim 21, further comprising  
2 incrementing the count if the login attempt is permissible but otherwise unsuccessful  
3 and is made with the password.

1 24. The login method of claim 21, further comprising  
2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined threshold  
4 and the login attempt is made with the password.

1 25. The login method of claim 21, further comprising  
2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined threshold  
4 within a third period of time and the login attempt is made with the password.

1 26. The login method of claim 21, wherein



- 1 34. The login method of claim 28, further comprising  
2 invalidating the subsequent login attempt if the count equals a predefined threshold  
3 and the user name is submitted with the subsequent login attempt.
- 1 35. The login method of claim 1, further comprising  
2 maintaining a count of unsuccessful login attempts to login from a network address.
- 1 36. The login method of claim 35, further comprising  
2 incrementing the count if the login attempt is impermissible and made from the  
3 network address.
- 1 37. The login method of claim 35, further comprising  
2 incrementing the count if the login attempt is permissible but otherwise unsuccessful  
3 and made from the network address.
- 1 38. The login method of claim 35, further comprising  
2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined threshold  
4 and the login attempt is made from the network address.
- 1 39. The login method of claim 35, further comprising  
2 selecting the second period of time by reference to the count, wherein the second  
3 period of time is longer than it otherwise would be if the count reaches a predefined threshold  
4 within a third period of time and the login attempt is made from the network address.
- 1 40. The login method of claim 35, wherein  
2 the second period of time is not increased as the count increases unless each of the  
3 defined number of unsuccessful login attempts to login from the network address occur  
4 within a third period of time.
- 1 41. The login method of claim 35, further comprising

invalidating the subsequent login attempt if the count equals a predefined threshold and the subsequent login attempt is made from the network address.

42. The login method of claim 1, wherein

the second period of time is a first length if the login attempt is one in a series of unsuccessful login attempts associated with the login token, which follow a successful attempt associated with the login token, if the series of unsuccessful login attempts does not include more than a predefined number unsuccessful login attempts;

the second period of time is a second length if the login attempt is one in a series of unsuccessful login attempts associated with the login token, which follow a successful attempt associated with the login token, if the series of unsuccessful login attempts includes the predefined number unsuccessful login attempts;

the second period of time is a third length if the login attempt does not follow a successful attempt associated with the login token, said third length exceeding the first length; and

the second period of time is a fourth length if the login token is not provided during the login attempt, said fourth length exceeding the first length.

43. The login method of claim 1, further comprising

processing a second login token, if provided, during a second login attempt, wherein the login cookie provided in response to the second login attempt does not permit a subsequent login attempt at least until the second period of time has expired twice since the login attempt.

44. A login method comprising

processing a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination;

providing a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts;

8 providing a second-class login token if the login attempt is unsuccessful and a login  
9 token submitted with the login request is second-class, wherein a subsequent login attempt  
10 made with said second-class login token is not permissible if submitted prior to expiration of  
11 a second time delay, said second time delay exceeding said first time delay;

12 providing the second-class login token if the login attempt is unsuccessful and is the  
13 last of a series of unsuccessful login attempts associated with a first-class login token, said  
14 series including more than the predefined number of unsuccessful login attempts; and

15 providing the second-class login token if a login token is not submitted with the login  
16 attempt, said login attempt not being permissible.

1 45. The login method of claim 44, wherein

2 the login attempt is not permissible if a login token submitted with said login attempt  
3 is invalid.

1 46. The login method of claim 44, wherein

2 the login attempt is not permissible if said login attempt is made prior to expiration of  
3 a time delay associated with a login token submitted with said login attempt.

1 47. A computer program product for use in conjunction with a computer system, the  
2 computer program product comprising a computer readable storage medium and a computer  
3 program mechanism embedded therein, the computer program mechanism comprising:

4 instructions for processing a login attempt to determine whether the login attempt is  
5 successful, said login attempt being successful if permissible and submitted with a valid user  
6 name and password combination;

7 instructions for providing a first-class login token if the login attempt is successful,  
8 said first-class login token permitting a predefined number of unsuccessful login attempts  
9 without imposing more than a first time delay between each of said unsuccessful login  
10 attempts;

11 instructions for providing a second-class login token if the login attempt is  
12 unsuccessful and a login token submitted with the login request is second-class, wherein a  
13 subsequent login attempt made with said second-class login token is not permissible if



submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay;

instructions for providing the second-class login token if the login attempt is unsuccessful and is the last of a series of unsuccessful login attempts associated with a first-class login token, said series including more than the predefined number of unsuccessful login attempts; and

instructions for providing the second-class login token if a login token is not submitted with the login attempt, said login attempt not being permissible.

48. A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for processing a login token, if provided, during an attempt to login, wherein the login attempt is impermissible if the login attempt occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token; and

instructions for providing an updated login token in response to the login attempt, wherein the updated login token does not permit a subsequent login attempt before expiration a second period of time if the login attempt is impermissible.

49. A computer system for processing login requests, comprising:

a first-class login server and a second-class login server, said first-class login server and said second-class login server each including a storage unit and a processor, said storage unit configured to store login information, said processor configured to process login requests with reference to said login information;

the first-class login server and the second-class login server each configured to process a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination;

the first-class login server configured to process login attempts made with a first-class login token and the second-class login server configured to process login attempts made with a second-class login token;

the first-class login server and the second-class login server each further configured to provide a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts;

the second-class login server further configured to provide a second-class login token if the login attempt is unsuccessful, wherein a subsequent login attempt made with said second-class login token is impermissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay; and

the first-class login server further configured to provide a second-class login token if the login attempt is unsuccessful and the login attempt is the last of a series of unsuccessful login attempts associated with a specific first-class login token, said series including more than the predefined number of unsuccessful login attempts.

50. The computer system of claim 49, wherein the second-class login server is further configured to serially process login attempts.

51. The computer system of claim 50, wherein the second-class server is further configured to process login attempts at a defined rate.

52. The computer system of claim 51, wherein the second-class server is further configured to decrease the defined rate in response to an occurrence of a set of unsuccessful login attempts.

53. The computer system of claim 51, wherein the second-class server is further configured to decrease the defined rate if a defined number of unsuccessful login attempts occur during a defined period of time.

54. The computer system of claim 53, wherein the second-class server is further configured to increase the defined rate if the defined number of unsuccessful login attempts do not occur during the defined period of time.

